AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for authenticating an electronic message containing message data and an electronic address, comprising the steps of:

receiving the electronic message from a sender;

creating a digest of the message data;

appending a temporal stamp and a unique value to the digest;

signing the digest, [[and]] the temporal stamp, and the unique value with a digital signature;

sending the digest, the temporal stamp, the unique value, and the digital signature to the electronic address as an electronic postmark~~, wherein the electronic postmark includes a value that uniquely identifies the electronic postmark~~;

authenticating the digest, the temporal stamp, the unique value, and the digital signature;

storing a copy of the digest, the temporal stamp, the unique value, and the digital signature in a log file; and

creating a digest of the log file.

2. (Original) The method of claim 1, where the step of creating a digest comprises generating a one-way hash value from the electronic message.

3. (Original) The method of claim 1, wherein the step of creating a temporal stamp comprises using the time and the date which indicate when the electronic message was received.

4. (Currently Amended) The method of claim 1, wherein the step of sending the digest, the temporal stamp, the unique value, and the digital signature comprises sending the electronic message.

5. (Previously Presented) The method of claim 1, wherein the electronic address is the electronic address of the sender.

6. (Original) The method of claim 4 wherein the step of sending the electronic message comprises attaching at least one legal protection of an official entity.

7. (Canceled)

8. (Previously Presented) The method of claim 1, further comprising the step of:

appending a temporal stamp to the digest of the log file; and

signing the digest of the log file and temporal stamp with a digital signature.

9. (Original) The method of claim 1 wherein the step of authenticating further comprises the steps of:

verifying that the digital signature was signed by the official entity;

verifying the specific identity of the entity which signed the digital signature; and

authenticating the contents of the electronic message using the digest.

10. (Currently Amended) A method for authenticating an electronic message containing data and an electronic address of a recipient, comprising the steps of:

sending an electronic message from a sender to a sender client;

receiving the electronic message at the sender client;

creating, by the sender client, a hash value from the data of the electronic message;

sending the hash value and the recipient electronic address from the sender client to an authentication server;

generating an electronic postmark data structure by the authentication server, the electronic postmark data structure including the hash value, item and date information, and a value that uniquely identifies the electronic postmark data structure;

sending the electronic postmark data structure and the recipient electronic address from the authentication server to a recipient client;

sending the electronic postmark data structure from the recipient client to a recipient at the recipient electronic address;

authenticating the electronic postmark data structure at the recipient;

storing a copy of the electronic postmark data structure in a log file; and

creating a digest of the log file.

11. (Original) The method of claim 10, wherein the step of generating an electronic postmark data structure includes generating a digital signature for inclusion in the electronic postmark data structure.

12. (Original) The method of claim 11, wherein the step of generating a digital signature includes generating a digital key.

13. (Original) The method of claim 12, wherein the step of authenticating the electronic postmark data structure includes using the digital key.

14. (Original) The method of claim 11, wherein the step of generating a digital key involves including the digital key with the digital signature.

15. (Original) The method of claim 10, wherein the step of sending the hash value includes using an authentication server, which is an electronic postmark server.

16. (Currently Amended) A method for requesting authentication of an electronic message, performed by a sender client, comprising the steps of:

receiving message data and a recipient electronic address from a sender;

creating a hash value from the message data;

establishing a connection with an authentication server;

sending the hash value, [[and]] the recipient electronic address, and a unique value, as an electronic postmark, ~~wherein the electronic postmark includes a value that uniquely identifies the electronic postmark,~~ to the authentication server;

sending an authentication request to the authentication server;

storing a copy of the hash value in a log file; and

creating a digest of the log file.

17. (Original) The method of claim 16, wherein the step of establishing a connection includes sender client and the authentication server using TCP/IP.

18. (Original) The method of claim 16, wherein the step of sending an authentication request includes requesting an electronic postmark data structure for the authentication.

19. (Original) The method of claim 18, wherein the step of establishing a connection with an authentication server includes using an electronic postmark server.

20. (Currently Amended) A method for receiving authentication of an electronic message, performed by a receiver client, comprising the steps of:

receiving a recipient electronic address and an electronic postmark data structure for the electronic message from an authentication server, the electronic postmark data structure including time and date information and a value that uniquely identifies the electronic postmark data structure;

sending the electronic postmark data structure to a recipient at the recipient electronic address;

storing a copy of the electronic postmark data structure including time and date in a log file: and

creating a digest of the log file.

21. (Original) The method of claim 20, wherein the step of receiving the electronic message involves communicating between the receiver client and the authentication server using TCP/IP.

22. (Original) The method of claim 20, wherein the step of receiving the electronic message from an authentication server involves using the authentication server which is an electronic postmark server.

23. (Original) The method of claim 20, further comprising the step of: verifying the electronic postmark data structure using a digital key.

24. (Original) The method of claim 23, wherein the step of verifying the electronic postmark data structure involves including the digital key with the electronic postmark data structure.

25. (Original) The method of claim 20, wherein the step of receiving a recipient electronic address and an electronic postmark data structure further includes the step of receiving the electronic message.

26. (Original) The method of claim 20, wherein the step of sending the electronic postmark data structure to a recipient further includes the step of sending the electronic message.

27. (Previously Presented) A method for authenticating an electronic message, performed by an authentication sever, comprising the steps of:

receiving a request to authenticate the electronic message, the request including a recipient electronic address and a hash value corresponding to the electronic message;

creating an electronic postmark data structure for the electronic message, the electronic postmark data structure including time and date information and a value that uniquely identifies the electronic postmark data structure;

generating a digital signature for the electronic postmark data structure; including the digital signature in the electronic postmark data structure;

generating a public digital key for a recipient;

exporting the public digital key to a key authenticator for authorizing;

sending the electronic postmark data structure and the recipient electronic address to a recipient client for delivery to the recipient at the recipient electronic address;

storing a copy of the electronic postmark data structure including the time and date information in a log file; and

creating a digest of the log file.

28. (Original) The method of claim 27, further comprising the steps of:

obtaining a authorized digital key for the electronic postmark data structure from a key authenticator, wherein the recipient can use the authorized digital key to verify the electronic postmark data structure; and

sending the authorized digital key to the receiver client.

29. (Original) The method of claim 27, wherein the step of receiving a request further involves including the electronic message in the request.

30. (Original) The method of claim 27, wherein the step of sending the electronic postmark data structure to a recipient client includes sending the electronic message to the recipient client.

31. (Previously Presented) The method of claim 27, wherein the step of exporting the public digital key to a key authenticator involves using one of a key signing authority and a certificate authority.

32. - 41. (Canceled)

42. (Previously Presented) A method for authenticating an electronic message, comprising the steps of:

sending a message comprising message data and a recipient electronic address from a sender to a sender front-end module at a sender client;

transmitting the message from the sender front-end module to a sender client proxy module at the sender client;

creating, by the sender client proxy module, a hash value from the message data;

sending the hash value and the recipient electronic address from the sender client proxy module via a network client module to a network server module at an authentication server;

generating an electronic postmark for the hash value by the authentication server, the electronic postmark including time and date information and a value that uniquely identifies the electronic postmark;

sending the electronic postmark and the recipient electronic address from the authentication server via a network client module on a recipient client to a recipient client proxy module on a recipient client;

transmitting the electronic postmark and the recipient electronic address from the recipient client proxy module to a recipient front-end module at the recipient client;

sending the electronic postmark from the recipient client to a recipient at the recipient electronic address;

storing a copy of the electronic postmark hash value in a log file; and

creating a digest of the log file.

43. (Original) The method of claim 42, wherein the step of generating an electronic postmark involves using the time and the date which indicate when the electronic message was received by the authentication server.

44. (Original) The method of claim 42, wherein the step of sending the hash value and the recipient electronic address to an authentication server involves using the authentication server which is an electronic postmark server.

45. (Original) The method of claim 42, further comprising the step of:

verifying the electronic postmark using a authorized digital key.

46. (Currently Amended) A system for authenticating an electronic message containing message data and an electronic address, comprising:

a receiver configured to receive the electronic message from a sender;

a digest component configured to create a digest of the message data;

a stamp component configured to append a temporal stamp to the digest;

a signing component configured to sign the digest and the temporal stamp with a digital signature;

a sender configured to send the digest, the temporal stamp, a unique value, and the digital signature to the electronic address as an electronic postmark~~, wherein the electronic postmark includes a value that uniquely identifies the electronic postmark~~;

an authenticating sever configured to authenticate the digest, the temporal stamp, the unique value, and the digital signature;

a database configured to store a copy of the digest, the temporal stamp, the unique value, and the digital signature in a log file; and

a log digest component configured to create a digest of the log file.